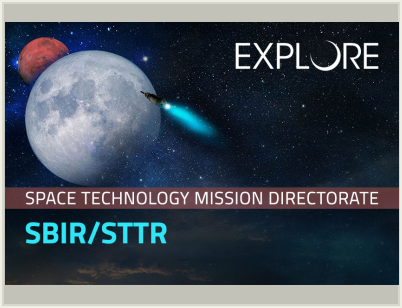
SAFE-P: System for Assurance of Flight Executable Procedures, Phase II

Completed Technology Project (2010 - 2013)

Project Introduction

NASA operates manned spacecraft according to rigorously-defined standard operating procedures. Unfortunately, operating procedures are often written in different languages. For example, Orion will use automatic procedures written in SCL, the Spacecraft Command Language, while backup manual procedures may be developed in PRL, the Procedure Representation Language. However, procedures developed in different languages may diverge, so that the backup PRL procedures do not operate in the same way as the SCL procedures. This could lead to unintended effects that may range from simply unexpected to inefficient or even catastrophic. We propose to develop the SAFE-P tool, which will use formal model-checking methods to prove that PRL and SCL procedures have the same underlying execution semantics. Our Phase 1 effort validated the effectiveness of our approach; Phase 2 will completely automate the model checking process and integrate with the Procedure Integrated Development Environment (PRIDE). SAFE-P will thus allow procedure authors to easily compare procedures as they are being developed. When differences are found by SAFE-P, they will be highlighted immediately in the PRIDE interface, allowing the operators to either fix problems or annotate the respective procedures to explain the differences. Using SAFE-P, NASA personnel will rapidly and confidently verify that if an automatic SCL program cannot be executed, a backup manual procedure in PRL will be equivalent and safe. Furthermore, as automatic translators are developed to transform procedures in one language into another NASA-relevant language (e.g., Tietronix's current effort to translate PRL into SCL), the SAFE-P tool will provide a critical validation mechanism to double-check the correctness of the translation and highlight areas where the translator makes mistakes (or deliberate approximations that yield different behavior).



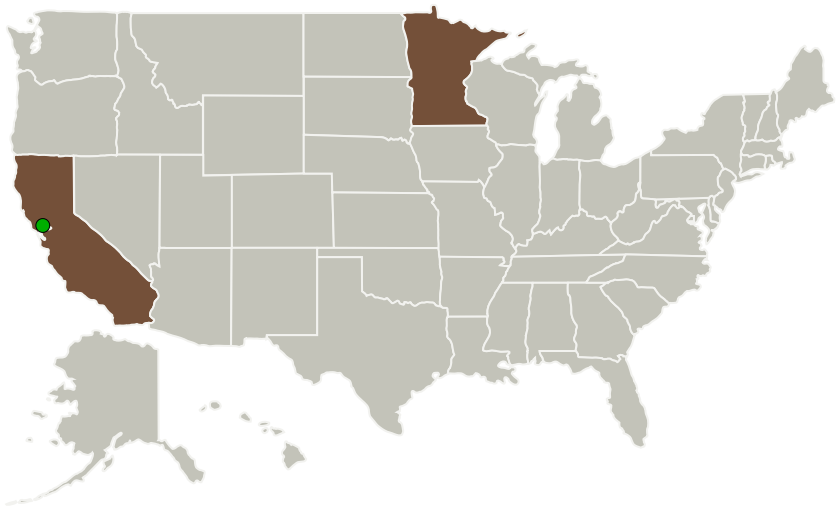
SAFE-P: System for Assurance of Flight Executable Procedures, Phase II

Table of Contents

SAFE-P: System for Assurance of Flight Executable Procedures, Phase II

Completed Technology Project (2010 - 2013)

Primary U.S. Work Locations and Key Partners



Organizations Performing Work	Role	Type	Location
SIFT, LLC	Lead Organization	Industry	Minneapolis, Minnesota
Ames Research Center(ARC)	Supporting Organization	NASA Center	Moffett Field, California

Primary U.S. Work Locations	
California	Minnesota

Project Transitions

February 2010: Project Start

February 2013: Closed out

Closeout Documentation:

- Final Summary Chart*(https://techport.nasa.gov/file/139421)*

Organizational Responsibility

Responsible Mission Directorate:

Space Technology Mission Directorate (STMD)

Lead Organization:

SIFT, LLC

Responsible Program:

Small Business Innovation Research/Small Business Tech Transfer

Project Management

Program Director:

Jason L Kessler

Program Manager:

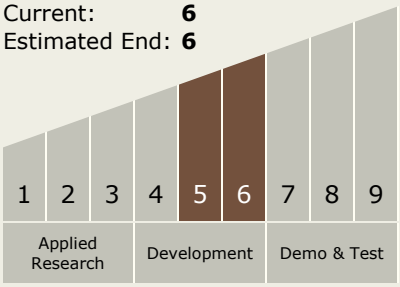
Carlos Torrez

Principal Investigator:

David J Musliner

Technology Maturity (TRL)

Start: **5**
Current: **6**
Estimated End: **6**



SAFE-P: System for Assurance of Flight Executable Procedures, Phase II

Completed Technology Project (2010 - 2013)

Technology Areas

Primary:

- TX11 Software, Modeling, Simulation, and Information Processing
  - TX11.1 Software Development, Engineering, and Integrity
    - TX11.1.5 Architecture and Design of Software systems

Target Destinations

The Sun, Earth, The Moon, Mars, Others Inside the Solar System, Outside the Solar System